The Internet & Television Association
25 Massachusetts Avenue, NW | Suite 100
Washington, DC 20001
(202) 222-2300

Danielle Piñeres
Associate General Counsel
o (202) 222-2459 e dpineres@ncta.com

January 4, 2017

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: Use of Spectrum Bands Above 24 GHz for Mobile Radio Services, GN Docket No. 14-177

Dear Ms. Dortch:

On January 4, 2017, NCTA – The Internet & Television Association (NCTA) submitted the attached comments to the Office of Management and Budget. We respectfully request that these comments be included in the record of the above-referenced proceeding. Please do not hesitate to contact me should you have any questions regarding this filing.

Respectfully submitted,

/s/ Danielle J. Piñeres

Danielle J. Piñeres

Attachment

The Internet & Television Association
25 Massachusetts Avenue, NW | Suite 100
Washington, DC 20001
(202) 222-2300

Danielle Piñeres
Associate General Counsel
o (202) 222-2459 e dpineres@ncta.com

January 4, 2017

VIA E-MAIL

Nicholas A. Fraser
The Office of Management and Budget
725 17th Street, N.W.
Washington, D.C. 20503
Nicholas_A._Fraser@omb.eop.gov

Cathy Williams
Federal Communications Commission
445 12th Street S.W.
Washington, D.C. 20554
Cathy.Williams@fcc.gov

Re: OMB Control No. 3060-1215; Use of Spectrum Bands Above 24 GHz for Mobile Radio Services, FCC 16-89

Dear Mr. Fraser and Ms. Williams:

NCTA – The Internet & Television Association (NCTA), the principal trade association representing the cable television industry in the United States, hereby submits comments in response to the Federal Communications Commission's (FCC) request for Office of Management and Budget (OMB) approval of the FCC's proposed data collection regarding the cybersecurity plans of 5G network operators.

In its 5G "spectrum frontiers" Report and Order (5G Order), the FCC adopted a rule requiring each Upper Microwave Flexible Use Service (UMFUS) licensee to file a public disclosure with the FCC describing its "plans for safeguarding [its] networks and devices from security breaches."[1] Every licensee must make this disclosure within three years of obtaining a license and at least six months before deploying its network. A senior executive must sign the report, which must describe, among other things, the licensee's: (1) approach to safeguarding the

---

[1] *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services, et al.*, Report and Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd 8014, 8104 ¶ 262 (2016) (*5G Order*).

confidentiality, integrity and availability of its network; (2) approach to mitigating cyber risk and the standards and practices employed to do so; (3) participation in industry organizations devoted to cybersecurity best practices; and (4) plans to incorporate outputs from Information Sharing and Analysis Organizations.[2]

As a procedural matter, the FCC's December 5th Public Notice (to which these comments respond) afforded interested parties their first opportunity to provide meaningful comment on the burden estimate associated with the 5G cybersecurity information collection.[3] The FCC's Notice of Proposed Rulemaking did not tee up the cybersecurity reporting requirement, and so this rule was not included in the package sent to OMB for pre-approval in January 2016.[4] After adopting the 5G Order, the FCC sought Paperwork Reduction Act (PRA) comment on the cybersecurity reporting requirement. However, the FCC provided only an overall burden estimate for all of the new information collections adopted in the 5G Order; it did not provide a breakout of the estimated burden of each specific new rule.[5] The supporting statement uploaded to OMB on December 1, 2016 provided the first indication by the FCC of its burden estimates specific to the 5G cybersecurity reporting rule.[6]

This rule creates a substantial new reporting burden that is not "necessary for the proper performance of the [FCC's] functions," and has no "practical utility."[7] The FCC's burden estimate also grossly understates the time and effort required to compile, review, and publish a public statement on a company's cybersecurity practices. For these reasons, OMB should not approve this information collection.

I. The FCC's 5G Cybersecurity Reporting Requirement Has No Practical Utility and Is Not Necessary for Performance of the FCC's Functions

The 5G cybersecurity reporting rule has no practical utility in advancing cybersecurity.[8] This is the case because requiring licensees to publicly disclose their network security plans will either: (1) produce reports that are at a high enough level of generality to avoid compromising network security by providing details that create vulnerabilities, but therefore offer the FCC

---

2 *Id.* at 8104-05 ¶ 263.

3 *See Information Collections Being Submitted for Review and Approval to the Office of Management and Budget*, 81 Fed. Reg. 87,556, 87,558 (Dec. 5, 2016).

4 *See generally* FCC, Supporting Statement, 3060-XXXX, *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services* (Jan. 13, 2016).

5 *See Information Collection Being Reviewed by the Federal Communications Commission*, 81 Fed. Reg. 65,358, 65,358 (Sept. 22, 2016).

6 FCC, Supporting Statement, 3060-1215, *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services*, at 9-10 (Dec. 1, 2016) (FCC Supporting Statement).

7 *See* 44 U.S.C. §§ 3506(c)(3)(A), 3508.

8 *See id.* § 3506(c)(3)(A).

information with no practical use; or (2) expose information that could reveal network risks and vulnerabilities, and thereby decrease the security of 5G networks and increase cybersecurity threats. In fact, if the public information submitted by network operators is truly so generic and high level that it does not create vulnerabilities, that information would be of little practical utility to the FCC in evaluating whether licensees have "engage[d] in the development of security measures at an earlier stage" or in "identifying security risks, including areas where more attention to security may be needed."[9] On the other hand, even the high-level information that the rule requires licensees to disclose may unintentionally reveal a vulnerability that bad actors could exploit.

The FCC has failed to explain how specifically it will use the information collected to advance its goals of ensuring that licensees incorporate security by design in their 5G networks and devices and identifying 5G security risks. The PRA implementing regulations note that the practical utility of an information collection must be "actual," not "merely the theoretical or potential," and the agency must demonstrate an "actual timely use for the information."[10] The FCC has failed to do so here.

This new reporting burden also is not necessary to the proper functioning of the FCC—even if the rule were to produce practically useful information, acting upon this information would likely exceed the FCC's authority. As several parties pointed out in their petitions for reconsideration of this rule, "Congress has not delegated cybersecurity regulatory authority to the FCC, focusing on the Department of Homeland Security . . . and other agencies to manage cybersecurity risk by emphasizing public-private partnerships."[11] Furthermore, as FCC Commissioner Ajit Pai explained in his separate statement, issued with the 5G Order, the FCC "lack[s] the expertise and authority to dive headlong into this issue, and . . . [no] agency should take a band-by-band approach to cyber. These are issues that are better left for security experts to handle in a more comprehensive way."[12]

Moreover, the FCC has failed to identify any persuasive reason that the information collected through this rule is necessary to the FCC's functions. The FCC imposes no such cybersecurity reporting requirements on mobile network operators in other bands and did not

---

9 *5G Order*, 31 FCC Rcd at 8104 ¶ 262.

10 5 C.F.R. § 1320.3(l).

11 Petition for Reconsideration of CTIA, GN Docket No. 14-177, IB Docket Nos. 15-256 & 97-95, RM-11664, and WT Docket No. 10-112, at 10-12 (filed Dec. 14, 2016); *see also* 5G Americas Petition for Reconsideration, GN Docket No. 14-177, IB Docket Nos. 15-256 & 97-95, RM-11664, and WT Docket No. 10-112, at 13-14 (filed Dec. 14, 2016).

12 *5G Order*, 31 FCC Rcd at 8279 (Statement of Commissioner Ajit Pai); *see also id.* at 8282 (Statement of Commissioner Michael O'Rielly) ("I don't think that this reporting requirement is necessary or all that helpful. Once again, this is the Commission gathering data for the purposes of monitoring, but it is really a means for the Commission to interfere in the design and operations of networks and the starting point for future regulation.").

demonstrate in the 5G Order that there are special security risks that justify singling out network operators using this specific set of frequencies for extra reporting burdens. The FCC also did not explain why this public cybersecurity report is necessary in light of existing public-private forums—including the National Institute of Science and Technology (which developed the business-driven Cybersecurity Framework), the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) (an advisory committee with several working groups tasked to work on pertinent cybersecurity-related issues), and the Communications Sector Coordinating Council and the Communications Sector Information Sharing and Analysis Center (public-private partnerships with the Department of Homeland Security, national security agencies, and law enforcement agencies)—that address best practices and facilitate the sharing of cyber threat information between the public and private sectors, and within the communications sector, particularly among mobile network providers.[13] Given the ongoing work in these existing forums, the FCC's reasoning that the cybersecurity reporting rule is necessary to "facilitate multi-stakeholder peer review and earlier development of devices and a commercially viable market for the service" is unpersuasive.[14]

II. The FCC Vastly Understates the Burden that the 5G Cybersecurity Reporting Requirement Would Impose on Licensees

The FCC estimates that each licensee required to file a 5G cybersecurity statement will expend five hours of attorney time (paid at an hourly rate of $66.88/hour) to prepare and file the report.[15] This estimate grossly understates the amount of time and money UMFUS network operators would spend in order to comply with the new cybersecurity reporting rule.

Based on our members' experience filing FCC reports, we estimate that licensees would

---

[13] *See, e.g.*, U.S. Dep't of Commerce - Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity*, at 1 (Feb. 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (describing how the NIST framework "us[es] business drivers to guide cybersecurity activities" and provides "a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors"); FCC, *Communications Security, Reliability and Interoperability Council V*, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability (last updated Dec. 23, 2016); The Commc'ns Security, Reliability and Interoperability Council IV, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*, at 31 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4 Final_Report_031815.pdf (recommending that the FCC "promote the voluntary use of the NIST CSF among all communications sector members"); U.S. Commc'ns Sector Coordinating Council, *FAQ: Why Should My Business Join the CSCC?*, http://www.comms-scc.org/faq/.

[14] *5G Order*, 31 FCC Rcd at 8105 ¶ 264.

[15] FCC Supporting Statement at 9-10.

spend far more than five hours preparing the cybersecurity disclosure, which would require the participation of multiple business units for each licensee. A network operator's technical, engineering, and operations teams would all be necessary to prepare a statement regarding cybersecurity practices. Because the issuance of a public statement on network security practices could establish a duty of care for network operators, and because the FCC's rule would explicitly require a senior executive to sign off, a company's legal department would also be involved in preparing, reviewing, and filing the report. Smaller companies that lack in-house expertise on these issues may incur the added expense of hiring outside counsel to assist in preparing the report.[16] A multi-departmental project of this scope ensures that a compliant cybersecurity statement cannot be prepared in anything close to five hours.

Furthermore, a cybersecurity disclosure would require companies to exercise extraordinary care. Such a public statement could simultaneously risk revealing competitively sensitive information and security vulnerabilities, while also subjecting a company to potential enforcement action. Because of the sensitive nature of the information involved and the potential for enforcement, such a statement would undoubtedly undergo multiple drafts and layers of review, adding time and complexity to compliance costs.

The FCC's burden estimate also assumes that network operators will submit only one report,[17] when the 5G Order clearly contemplates additional filings. Specifically, the 5G Order states that "[t]o the extent that there are material changes to the information presented in the Statement, licensees must file updates to notify the Commission."[18] Because 5G technology is still in the nascent stages of development, a new licensee's network security plans may remain dynamic for some time after it acquires a license, necessitating multiple "update" filings with the FCC. The FCC's burden estimate inappropriately fails to account for the burden associated with the regular update filings contemplated in the 5G Order.

---

[16] The FCC's estimate of $66.88/hour for in-house attorney time itself appears very low, but note that hiring expert outside regulatory compliance counsel would almost certainly cost hundreds of dollars per hour. *See, e.g.*, *Billing Rates Across the Country*, THE NAT'L LAW J. (Jan. 13, 2014), http://www.nationallawjournal.com/id=1202636785489/Billing-Rates-Across-the-Country (indicating that the average annual billing rate is $370 per hour for a law firm associate); Major, Lindsey & Africa, *2014 Partner Compensation Survey*, at 48 (2014), https://www.mlaglobal.com/publications/research/compensation-survey-2014 (indicating that the average billing rate for a Washington, D.C. law firm partner is $705/hour).

[17] *See* FCC Supporting Statement at 9-10.

[18] *5G Order*, 31 FCC Rcd at 8104 n.673.

III. Conclusion

As discussed above, the public 5G cybersecurity reporting requirement has no practical utility, is not necessary to the FCC's functions, and using information contained in the reports could exceed the FCC's Congressionally defined authority. Moreover, the FCC has substantially understated the burden that this new information collection would impose on network operators. For these reasons, NCTA respectfully requests that OMB not approve this information collection.

Respectfully submitted,

/s/ Danielle J. Piñeres

_____

Rick Chessen
Danielle J. Piñeres
NCTA – The Internet & Television Association
25 Massachusetts Avenue, NW – Suite 100
Washington, DC 20001-1431
(202) 222-2445